Goddard Space Flight Center
Protective Services Contract
NNG12364774R

ATTACHMENT M

DD 254

Dated: 3/9/12

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION

(The requirements of the DoD Industrial Security Manual apply To all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING

a. FACILITY CLEARANCE REQUIRED: Secret

b. LEVEL OF SAFEGUARDING REQUIRED: None

2. THIS SPECIFICATION IS FOR: (X and complete as applicable)			**3. THIS SPECIFICATION IS:** (X and complete as applicable)			
X	a. PRIME CONTRACT NUMBER		X	a. **ORIGINAL** (Complete date in all cases)		Date (YYMMDD)
	b. SUBCONTRACT NUMBER			b. **REVISED** (Supersedes all previous specs)	Revision No.	Date (YYMMDD)
	c. SOLICITATION OR OTHER	Due Date (YYMMDD)		**FINAL** (Complete Item 5 in all cases)		Date (YYMMDD)

4. IS THIS A FOLLOW-ON CONTRACT? [ ] YES [X] NO. If Yes, complete the following:

Classified material received or generated under _____ (Preceding Contract Number) are transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? [ ] YES [X] NO. If Yes, complete the following:

In response to the contractor's request dated _____, retention of the classified material is authorized for the period _____

6. CONTRACTOR (Include Commercial and Government Entity (CAGE) Code)

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE	c. COGNIZANT SECURITY OFFICE (Name, Address, and Zip
NASA/Goddard Space Flight Center Greenbelt, MD 20771		NASA/Goddard Space Flight Center Greenbelt, MD 20771

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

Protective Services at Goddard Space Flight Center (GSFC), Wallops Flight Facility (WFF), Independent Verification and Validation Facility,(IV&V) and Goddard Institute for Space Sciences (GISS).

10.CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION		X
b. RESTRICTED DATA		X
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION		X
d. FORMERLY RESTRICTED DATA		X
e. INTELLIGENCE INFORMATION		
(1) Sensitive Compartmented Information (SCI)		X
(2) Non-SCI	X	
f. SPECIAL ACCESS INFORMATION		X
g. NATO INFORMATION		X
h. FOREIGN GOVERNMENT INFORMATION		X
i. LIMITED DISSEMINATION INFORMATION	X	
j. FOR OFFICIAL USE ONLY INFORMATION	X	
k. OTHER (Specify)		X

11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR	YES	NO
a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY	X	
b. RECEIVE CLASSIFIED DOCUMENTS ONLY		X
c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		X
d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		X
e. PERFORM SERVICES ONLY		X
f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		X
g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		X
h. REQUIRE A COMSEC ACCOUNT		X
i. HAVE TEMPEST REQUIREMENTS		X
j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		X
k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		X
l. OTHER (Specify)		

12. PUBLIC RELEASE Any information (classified or unclassified) pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release

[X] Direct [ ] Through (Specify)

NASA/GODDARD SPACE FLIGHT CENTER 130/OFFICE OF PUBLIC AFFAIRS GREENBELT, MD 20771

CC To the Public Affairs Division, NASA Headquarters, Washington, D.C. 20546 for review.

13. SECURITY GUIDANCE. The security classifiection guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. (Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)

In performance of this contract, some personnel may require access to classified information up to the SECRET level. The contractor must have sufficient number of cleared employees assigned duties under this contract to be able to complete all classified work assignments up to and including SECRET.

1. DoD 5220.22-M, National Industrial Security Program Operating Manual, February 28, 2006
2. NPR 1600.1, NASA Security Program Procedural Requirements w/Change 2, April 1, 2009
3. NPD 1600.2E, NASA Security Policy, April 28, 2004 (Revalidated 4/1/2009)
4. NPR 2810.1A, Security of Information Technology, May 16, 2006
5. NPD 2810.1D, NASA Information Security Policy, May 9, 2009
6. GPR 1600.1, Goddard Security Requirements, April 3, 2008
7. NPD 1660.1B, NASA Counterintelligence (CI) Policy, November 18, 2008
8. NPR 1600.1, Counterintelligence (CI)/Counterterrorism (CT) Procedural Requirements, December 21, 2004
9. OMB Circular A-130, Management of Federal Information Resources
10. Federal Information Security Management Act of 2002
11. FOUO Information Attachment to DD-254

Any employee who observes or becomes aware of the deliberate or suspected compromise of classified national security information shall promptly report such information personally to the GSFC Counterintelligence (CI) Office. If unclassified but sensitive information appears compromised by or on behalf of foreign or domestic powers, organizations or persons, employees shall report such information to the GSFC CI Office. If an employee becomes aware of information pertaining to international or domestic terrorist activities, employees shall also report to the GSFC CI Office. If the information indicates a computer compromise or other cyber intrusion, the Office of Inspector General shall be promptly notified.

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. (If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement whch identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.) [ ] Yes [X] No

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. (If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.) [ ] Yes [X] No

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a.TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE (Include Area Code)
Jacquelyn R. Hogan	Industrial Security Specialist	301-286-5387

d. ADDRESS (Include Zip Code)	e. SIGNATURE
NASA Goddard Space Flight Center Code 240 Greenbelt, MD 20771	

17. REQUIRED DISTRIBUTION

[X]	a. CONTRACTOR
[ ]	b. SUBCONTRACTOR
[X]	c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
[ ]	d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
[X]	e. ADMINISTRATIVE CONTRACTING OFFICER
[ ]	f. OTHERS AS NECESSARY

FOUO ATTACHMENT TO DD FORM 254

FOR OFFICIAL USE ONLY (FOUO) INFORMATION HANDLING INSTRUCTIONS

1. GENERAL

1.1 FOR OFFICIAL USE ONLY (FOUO) is official government information that does not meet requirements for classification but still requires protection.

1.2 FOUO information may be withheld from the public under exemptions 2 through 9 of the Freedom of Information Act (5 USC 552). Most FOUO information generated or handled in support of this contract will be exempt from mandatory disclosure under exemptions 4 and 5.

1.3 FOUO information may be released to the public, however, it must be reviewed by the Government prior to its release. Information in support of this contract must be reviewed by SMC/AXP or SMC/PA prior to release.

2. IDENTIFICATION MARKINGS.

2.1 An unclassified document containing FOUO information will be marked "FOR OFFICIAL USE ONLY" on the outside of the front cover (if any), on the first page, on each page containing FOUO information, on the back page, and on the outside back cover (if any). For convenience, all pages, even those that do not contain FOUO information, may be marked in documents generated by automated systems.

2.2 Individual portions/paragraphs in unclassified documents that contain FOUO information may be marked "FOUO" to alert users and assist in reviews.

2.3 Individual pages within a classified document that contain both FOUO and classified information will be marked top and bottom with the highest security classification of information appearing on the page. Individual portions/paragraphs containing FOUO information but no classified information will be marked "FOUO".

2.4 The cover or the first page of unclassified documents containing FOUO information will be marked with the following statement:

This Document contains information
EXEMPT FROM MANDATORY DISCLOSURE
UNDER THE FOIA
EXEMPTIONS (b)(4) and (b)(5) apply

2.5 Certain classified material on this contract may be downgraded by the Original Classification Authority to UNCLASSIFIED-FOUO or may be automatically declassified under E.O. 12958. When classified material approved for declassification to U-FOUO is used, extracted, reissued, transmitted and/or updated, it must be reviewed and appropriately marked.

3. TRANSMISSION/DISSEMINATION/REPRODUCTION

3.1 Authorized contractors, consultants, and grantees may transmit/disseminate FOUO information internally to each other and to DOD components and officials of DOD components who have a legitimate need for the information in connection with this contract. The following guidelines apply:

3.1.1. FOUO information may be discussed over non-secure telephones and other electronic instruments. Cordless, cellular, and mobile telephones should be avoided.

3.1.2. FOUO information may be transmitted over non-secure facsimile equipment.

3.1.3. Documents of facsimile transmissions containing FOUO material or with FOUO material attached must be marked to identify any FOUO contents or attachments.

3.1.4. FOUO information may be sent via U.S. Postal Service of commercial carrier as long as the shipping package is not marked as containing FOUO material.

3.1.5. FOUO information may be transmitted, processed, and stored on Automated Information Systems (AIS), electronic mail, and other similar systems or networks 1) when distribution is to an authorized recipient and 2) if the receiving system is protected by either physical isolation or a password protection system. Holders will not use general, broadcast, or universal mail addresses to distribute FOUO information. Discretionary access control measures may be used to preclude access to FOUO files by users who are authorized system users but are not authorized for FOUO information.

3.1.6. Reproduction of FOUO information may be accomplished on unclassified copiers or within designated government or contractor reproduction areas.

4. STORAGE

4.1 During working hours, FOUO information shall be used in a manner that limits access by persons who do not have an official need for the information. During non-working hours and when internal building security is provided, FOUO

material may be filed with other unclassified records in unlocked files or desks. When there is no internal building security, locked buildings or rooms will provide adequate after-hours protection, or the material can be stored in locked receptacles such as file cabinets, desks, or bookcases.

5. DISPOSITION

5.1 When no longer needed, FOUO information should be disposed of in a manner to hinder reconstruction, e.g. by shredding or tearing each sheet into pieces and placing in a recycle or trash container by initializing, degaussing, or shredding magnetic media.

5.2 FOUO material may be recycled. Safeguard the FOUO documents or information until recycled. Recycling contracts must include agreements on how to protect and destroy FOUO material.

5.3 Removal of the FOUO status can only be accomplished by the government originator of the information. SMC/AXP or SMC/PA will review and/or coordinate the removal of FOUO status for information in support of this contract.

6. UNAUTHORIZED DISCLOSURE

6.1 Government and contractor personnel must act to protect FOUO information under their control from unauthorized disclosure. Government and contractor organizations must inform SMC/AXP or SMC CZ of any unauthorized disclosures of FOUO information in support of this contract. Unauthorized disclosure, intentional disregard, or gross negligence in the handling of FOUO information does not constitute a reportable National Security Information violation under the NISPOM. However, the responsible organization should investigate and, when substantiated, take appropriate disciplinary action. Unauthorized disclosure of FOUO information containing Privacy Act information may also result in civil or criminal sanctions.